

Bellovin 113031

IN THE CLAIMS:

**Claim 1 (Currently Amended):** A method executed within a processing unit for filtering packets, comprising the steps of:

receiving a packet that includes an encrypted identifier for verifying identity of a first device that sent said packet, while remainder of said packet unencrypted sent from a first device to a second device;

authenticating an said identifier for said packet;

determining whether to send forward said packet to said a second device based on result of said authenticating, and a policy relative to said source device; and

sending forwarding said packet to said second device in accordance with said determination.

**Claim 2 (Currently Amended):** The method of claim 1, wherein said step of determining comprises:

comparing said- authenticated identifier yielded by said step of authenticating to a list of identifiers;

retrieving at least one policy rule relative to said authenticated identifier;

determining whether to send said packet to said second device in accordance with said comparison and said policy rule.

**Claim 3 (Delete) .**

**Claim 4 (original):** The method of claim 1, wherein said authenticating is performed in accordance with IPSEC standards.

**Claim 5 (original):** The method of claim 1, wherein said authenticating comprises:

retrieving a pointer to a security association from an authentication header from said packet;

retrieving a key associated with said security association; and

determining whether said packet is authentic using said key.

Bellovin 113031

**Claim 6 (Currently Amended):** The method of claim 5, further comprising the step of  
~~wherein said identifier is not authentic, further comprising~~ sending a first message to a  
third device indicating said identifier is not authentic when said step of authenticating so  
determines.

**Claim 7 (original):** The method of claim 5 wherein said authentication header is an  
IPSEC authentication header.

B<sup>2</sup> **Claim 8 (Currently Amended):** The method of claim 1, wherein said packet is, in  
addition, encrypted ~~prior to said receiving, and said method further comprises~~  
decrypting said packet prior to authenticating.

**Claim 9 (original):** The method of claim 8, wherein said packet is encrypted and  
decrypted using one of group of cryptographic techniques comprising DES, triple  
DES, HMAC and RSA.

**Claim 10 (Currently Amended):** The method of claim 1, wherein said policy rule  
is stored in a policy configuration file at said processing unit.

**Claim 11 (Currently Amended):** A machine-readable memory whose contents  
cause a computer system to perform packet filtering, by performing the steps of:  
receiving a packet that includes an encrypted identifier for verifying identity of a  
first device that sent said packet, while remainder of said packet unencrypted sent from a  
~~first device to a second device;~~  
authenticating an said identifier for said packet;  
determining whether to send forward said packet to said a second device based on  
result of said authenticating, and a policy relative to said source device; and  
sending forwarding said packet to said second device in accordance with said  
determination.

Bellovin 113031

**Claim 12 (original):** The machine-readable memory of claim 11, wherein said determining comprises:

B2  
comparing said authenticated identifier yielded by said step of authenticating to a list of identifiers;

retrieving at least one policy rule relative to said authenticated identifier;

determining whether to send said packet to said second device in accordance with said comparison and said policy rule.

**Claim 13 (Delete) .**

**Claim 14 (original):** The machine-readable memory of claim 11, wherein said authenticating is performed in accordance with IPSEC standards.

**Claim 15 (original):** The machine-readable memory of claim 11, wherein said authenticating comprises:

retrieving a pointer to a security association from an authentication header from said packet;

B3  
retrieving a key associated with said security association; and determining whether said packet is authentic using said key.

**Claim 16 (Currently Amended):** The machine-readable memory of claim 15, further comprising the step of wherein said identifier is not authentic, further comprising sending a first message to a third device indicating said identifier is not authentic when said step of authenticating so determines.

**Claim 17 (original):** The machine-readable memory of claim 15 wherein said authentication header is an IPSEC authentication header.

**Claim 18 (Currently Amended):** The machine-readable memory of claim 11, wherein said packet is, in addition, encrypted prior to said receiving, and said method further comprising decrypting said packet prior to authenticating.

Bellovin 113031

**Claim 19 (original):** The machine-readable memory of claim 18, wherein said packet is encrypted and decrypted using one of group of cryptographic techniques comprising DES, triple DES, HMAC and RSA.

**Claim 20 (Currently Amended):** The machine-readable memory of claim 11, wherein said policy rule is stored in a policy configuration file at said processing unit.

**Claim 21 (Currently Amended):** A packet filter for a distributed firewall, comprising:  
an input means coupled to said first network for receiving a data packet from a first device, said data packet having an encrypted common host identifier for verifying identity of a first device that sent said packet via a decryption process, while remainder of said packet unencrypted;

a first buffer coupled to said input means for storing said received packet;

a first memory segment containing a list of common host identifiers and at least one policy rule;

a second memory segment for storing a program for decrypting said common host identifier, authenticating said common host identifier, and determining whether to send said packet to a second device based on said list and said policy rule;

a processor coupled to said first buffer, said first memory segment and said second memory segment for executing said program; and

an output means coupled to said first buffer for forwarding said compared data packet to said second device based on said comparison.

**Claim 22 (Previously amended):** The apparatus of claim 21, further comprising a second buffer for storing said compared data packet prior to forwarding said compared data packet to the second device.

**Claims 23 (Previously cancelled).**

**Claims 24 (Previously cancelled).**

Bellovin 113031

Claims 25 (Previously cancelled).

Claims 26 (Previously cancelled).

Claims 27 (Previously cancelled).

Claims 28 (Previously cancelled).

**Claim 29 (Currently Amended):** A distributed firewall system, comprising:

a first network device;

a second network device in communication with said first network device;

a packet filter processor for each network device;

B4  
an encryption means coupled to said packet filter processor, said encryption means for ~~decrypting and authenticating source of~~ a packet sent ~~between~~ from said first network device ~~said to~~ second network device by decrypting an encrypted portion of said packet; and

a system management module to manage said packet filter processors.

**Claim 30 (Previously added):** The system of claim 29 wherein said authenticating comprises:

B5  
retrieving a pointer to a security association from an authentication header from said packet;

retrieving a key associated with said security association; and

determining whether said packet is authentic using said key.

**Claim 31 (Previously added):** The system of claim 30 wherein said authentication header is an IPSEC authentication header.